REMARKS

Initially, in the Office Action dated July 5, 2005, the Examiner has rejected claims 24-27 under 35 U.S.C. §101. Further, claims 1 and 5 have been rejected under 35 U.S.C. §112, second paragraph. Claim 1 has been rejected under 35 U.S.C. §112, second paragraph. Claim 20 has been rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,282,193 (Hluchyj et al). Claims 1-8, 9, 11-14, 15-18 and 24-27 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Rigney et al RFC 2138 (RFC 2138) in view of Rigney et al RFC 2139 (RFC 2139). Claim 11 has been rejected under 35 U.S.C. §103(a) as being unpatentable over RFC 2138 in view of RFC 2139 and further in view of U.S. Patent No. 6,088,799 (Morgan et al).

The Examiner has indicated that claims 3-7, 10, 19 and 21-23 are objected to as being dependent upon a rejected base claim, but would be allowable if written in independent form, including all of the limitations of the base claim and any intervening claims.

By the present response, Applicant has amended claims 1, 3, 5, 7, 9, and 11 to further clarify the invention. Further, Applicant has canceled claims 24-27 without disclaimer. Claims 1-23 remain pending in the present application.

Allowable Subject Matter

Applicant thanks the Examiner for indicating that claims 3-7, 10, 19 and 21-23 would be allowable if rewritten in independent form, including all of the limitations of the base claim and any intervening claims.

35 U.S.C. §101 Rejections

Claims 24-27 have been rejected under 35 U.S.C. §101. Applicant has canceled these claims, therefore rendering these rejections moot.

35 U.S.C. §112 Rejections

Claims 1 and 5 have been rejected under 35 U.S.C. §112, second paragraph. Applicants have amended these claims to further clarify the invention and respectfully request that these rejections be withdrawn.

Claim 1 has been rejected under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential elements. Applicant has amended this claim to further clarify the invention and respectfully requests that this rejection be withdrawn.

35 U.S.C. §102 Rejections

Claim 20 has been rejected under U.S.C. §102(e) as being anticipated by Hluchyj et al. Applicant respectfully traverses this rejection.

Hluchyj et al discloses a remote access server in a packet network that includes a packet switch fabric, a packet network server and a dial access server. The packet network server has a first port for sending and receiving packet-based signals with the packet switch fabric and a second port for sending and receiving packet-based signals with the packet network. The dial access server has a port for sending and receiving packet-based signals with the packet switch fabric and the dial access server has a first digital signal processor for performing signal

processing on the packet-based signals. The packet switch fabric transfers packet-based signals among the packet network server, and the dial access server.

Regarding claim 20, Applicant submits that Hluchyj et al does not disclose or suggest the limitations in the combination of this claim of, *inter alia*, processing an access-request message at a message receiving point that includes authenticating the access-request message prior to performing user authentication of the access-request message such that abnormal access-request messages are not processed for user authentication. The Examiner asserts that these limitations are disclosed in Hluchyj et al at column 3, lines 49-57 and column 6, lines 1-19. However, these portions of Hluchyj et al merely disclose that "packet protocol processing" includes the information disclosed in RFC 1144 TCP header compression, along with support for user authentication and user's surface profile determination, and that the dial access server connects a packet bus through a packet bus interface, details on the dial access server, and detail processing of an analog modem call and an ISDN modem call. This is not authenticating an access-request message prior to performing user authentication of the access-request message such that abnormal access-request messages are not processed for user authentication, as recited in the claims of the present application. These portions of Hluchyj et al merely relate to a definition of packet protocol processing, and the processing performed by the dial access server and packet bus interface. Hluchyj does not disclose or suggest anything related to authenticating a message or authenticating a message prior to authenticating a user.

Accordingly, Applicants submit that Hluchyj does not disclose or suggest the limitations in the combination of claim 20 of the present application. Applicant respectfully requests that these rejections be withdrawn and that these claims be allowed.

35 U.S.C. §103 Rejections

Claims 1, 2, 8, 9, 11-14, 15-18 and 24-27 have been rejected under 35 U.S.C. §103(a) as being unpatentable over RFC 2138 in view of RFC 2139. Applicant respectfully traverses these rejections.

RFC 2138 entitled remote authentication dial-in user servers (RADIUS) discloses a protocol for carrying authentication, authorization, and configuration information between a network access server which desires to authenticate its links and a shared authentication server. A network access server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response which is returned. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver a service to the user. A RADIUS can act as a proxy client to other RADIUS servers or other kinds of authentication servers. Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. Any user passwords are sent encrypted between the client and RADIUS server, to eliminate the possibility that someone snooping on an unsecured network could determine a user's password.

RFC 2139 relates to RADIUS accounting and discloses a protocol for carrying accounting information between a network access server and a shared accounting server. A network access server operates as a client of the RADIUS accounting server. The client is responsible for passing the user accounting information to a designated RADIUS accounting server. The RADIUS accounting server is responsible for receiving the accounting requests and returning a response to the client indicating that it has successfully received the request.

Regarding claims 1, 9 and 17, Applicant submits that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of these claims of, *inter alia*, executing an encryption algorithm using the access-request message having the temporary authenticator value and the encrypted user password to generate a message digest, the access-request message having an authenticator field that is filled with a prescribed value, or generating a final access-request message by replacing the value of the authenticator field with the message digest, or transmitting the final access-request message to an authentication, authorization and accounting server, or processing the access-request message if the access-request message is successfully verified, or performing user authentication by decrypting an encrypted user password of the process access-request message using a temporary authenticator value of the processed access-request message and a shared secret key that is known to each of a message transmitter and a message receiver.

The Examiner asserts that RFC 2138 discloses transmitting the final access-request message to an AAA server on page 6 with the disclosure of receiving the request. However, these portions of RFC 2138 merely disclose that once the RADIUS server receives the request, it validates the sending client. This is not transmitting a final access-request message to an AAA server, the final access-request message being generated using the access-request message and replacing the value of the authenticator field with the message digest, or verifying the access-request message by the AAA server, as recited in the claims of the present application. RFC 2138 merely discloses a request for authentication from a client being received and validation of the sending client. In contrast, the limitations in the claims of the present application relate to transmitting a final access-request message including a message digest, and also verifying the access-request message.

The Examiner admits that RFC 2138 does not disclose or suggest executing an encryption algorithm to generate a message digest and filling in fields of a request message, but asserts that RFC 2139 discloses these limitations on page 5 with the disclosure of the request authenticator and MD5 hash placed in authenticator field. However, these portions of RFC 2139 merely disclose that in accounting-request packets, the authenticator value in the authenticator field of a RADIUS data format is a 16 octet MD5 checksum called the request authenticator and details on how the MD5 hash is calculated. This is not using the access-request message having the temporary authenticator value and the encrypted user password to generate a message digest,

as recited in the claims of the present application. Further, these portions of RFC 2139 (or RFC 2138) do not disclose or suggest the access-request message having an authenticator field that is filled with a prescribed value. These portions of RFC 2139 merely disclose that an MD5 hash function is performed and the resulted value stored in the authenticator field of the accounting-request packet. In contrast, the limitations in the claims of the present application relate to executing an encryption algorithm using the access-request message to generate a message digest. Further, neither RFC 2139 nor RFC 2138, disclose or suggest generating a final access-request message by replacing the value of the authenticator field with the message digest.

Moreover, the Examiner asserts that RFC 2138 discloses decoding the access-request message if the access-request message is successfully verified on page 6 by the disclosure of validates sending client. However, as noted previously, these portions of RFC 2138 merely disclose that once the RADIUS server receives the request, it validates the sending client. This is not processing the access-request message if the access-request message is successfully verified, as recited in the claims of the present application. These portions of RFC 2138 merely disclose that after receiving the request, the sending client is validated. In contrast, the limitations in the claims of the present application relate to processing the access-request message after the message is successfully verified. Further, none of the cited references disclose or suggest performing user authentication by decrypting an encrypted user password of the processed access-request message using a temporary authenticator value of the processed access-request

message and a shared secret key that is known to each of a message transmitter and a message receiver, as recited in the claims of the present application. The Examiner fails to provide any portion of any cited reference that discloses or suggests these limitations in the claims of the present application.

Regarding claims 2, 8, 11-14, 15, 16 and 18, Applicant submits that these claims are dependent on one of independent claims 1, 9 and 17 and, therefore, are patentable for the same reasons noted previously regarding these independent claims. For example, Applicant submits that none of the cited references disclose or suggest where the prescribed value is a value previously defined between a foreign agent and the AAA server, or where the randomly generated authenticator value is created differently every time a message is generated, or where the temporary authentication value is randomly generated each time a new access-request message is generated such that the temporary authenticator value is not known beforehand.

Accordingly, Applicant submits that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 1, 2, 8, 9, 11-14 and 15-18 of the present application. Applicant respectfully request that these rejections be withdrawn and that these claims be allowed.

Claim 11 has been rejected under U.S.C. 35 §103(a) as being unpatentable over RFC 2138 in view of RFC 2139 and further in view of Morgan et al. Applicant respectfully traverses this rejection.

Morgan et al discloses a process in which a user enters ID and password information at a network client computer terminal. This information is combined with an asymmetric key stored in a persistent storage directly accessible to the client's computer terminal. This combined information is communicated through a communication network to one or more server computers for authentication of the client. A similar identification and authentication process may be used to authenticate the server computer. Upon authentication of the client, the server provides the client computer with three symmetric keys in encrypted format, for encrypting and decrypting persistent information associated with the client's computer control program and associated with the log in ID, and used to encrypt and decrypt communication between the client computer and the server computer, respectively.

Applicant submits that claim 11 is dependent on independent claim 9 and, therefore, is patentable at least for the same reasons noted previously regarding this independent claim. Applicant submits that Morgan et al does not overcome these substantial defects noted previously regarding RFC 2138 and RFC 2139. For example, Applicant submits that none of the cited references disclose or suggest where the performing user authentication includes: decrypting the encrypted user password written in an attribute field of the decoded access-request message using the temporary authenticator of the decoded access-request message, comparing the encrypted user password and a user password stored in a database, determining that the user authentication is successful if the decrypted user password and the stored user

password are identical to each other, and determining that the user authentication has failed if the decrypted user password and the stored user password are not identical to each other.

Accordingly, Applicant submits that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of claim 11 of the present application. Applicant respectfully requests that this rejection be withdrawn and that this claim be allowed.

CONCLUSION

In view of the foregoing amendments and remarks, Applicant submits that claims 1-23 are now in condition for allowance. Accordingly, early allowance of such claims is respectfully requested. If the Examiner believes that any additional changes would place the application in better condition for allowance, the Examiner is invited to contact the undersigned, Frederick D. Bailey, at the telephone number listed below.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this, concurrent and future replies, including extension of time fees, to Deposit Account 16-0607 and please credit any excess fees to such deposit account.

Respectfully submitted,
FLESHNER & KIM, LLP

Carl R. Wesolowski
Registration No. 40,372
Frederick D. Bailey
Registration No. 42,282

P.O. Box 221200
Chantilly, Virginia 20153-1200
(703) 766-3701 JCE/FDB:cah:tlg
Date: December 5, 2005
\\fk4\Documents\2000\2000-122\78330.doc
Please direct all correspondence to Customer Number 34610